

**METHOD AND SYSTEM FOR PROVIDING
A SECURE MULTIMEDIA PRESENTATION**

Copyright Notice

A portion of the disclosure of this patent document contains material which is subject to copyright protection. The owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

Background of the Invention

Synchronized combinations of audio, video, raster still images and graphics, vector motion and still images and graphics, HTML, hyperlinks, Rich Text and other text are generically referred to as video clips. Through digitization, the electromagnetic signals which are used to represent each of these video clip components may be reduced to binary data files. These files may be stored in encrypted combinations as an encrypted video clip data file, encrypted in its entirety, and may be transferred to and decrypted and displayed by display units and other devices which are capable of decrypting and processing for display and playback of the encrypted video clip data file which contains the encrypted multimedia presentation.

One way of distributing the encrypted video clip data involves placing encrypted video clip data files on file servers which are accessible to users of

1 digital computer systems through channels such as the Internet and analogous
2 subscription network services. Alternate distribution and transmission methods
3 include radio frequencies (RF) and other such broadcast frequencies and
4 distribution methods such as those used by analog and digital radio and
5 television, cellular phones, and personal data assistants (PDAs) for playback and
6 decryption of the multimedia presentation on these and other such wireless
7 reception devices. Ideally, such users could locate the encrypted video clip data
8 file, discern the data formats of the encrypted video clip data components by the
9 data identifier and its unique file extension as an encrypted multimedia
10 presentation data file, receive the file and decrypt, process and playback the
11 video clip data on their digital computer systems and other devices with a CPU,
12 output display and audio capabilities to achieve display and interactive playback
13 of the video clip as a decrypted and secure multimedia presentation.

14 However, to date there exists no organized system for facilitating the
15 identification, distribution, transmission and playback of the data formats of the
16 encrypted component data files which are comprised and stored within the
17 encrypted multimedia presentation data file, nor is there presently a digital
18 computer system based and automatically decrypting video clip display unit
19 which is capable of providing a coherent and synchronized display of the
20 combination of decrypted audio, decrypted video, decrypted still raster images
21 and graphics, decrypted still and motion vector images and graphics, decrypted
22 HTML, decrypted Rich Text, decrypted hyperlinks, decrypted password data,

1 decrypted date expiration data and decrypted text represented by the data
2 contained in such a an encrypted video clip data file.

4 **Summary of the Invention**

5 The present invention is intended to overcome the obstacles inherent in
6 the state of the art and to provide users of digital computer systems and other
7 devices with a CPU and display and audio capabilities, with the ability to access
8 server-based encrypted video clips in a single multimedia presentation
9 transmission file which contains encrypted audio, video, still raster images and
10 graphics, still and motion vector images and graphics, HTML, Rich Text,
11 hyperlinks, password data, date expiration data, text and other textual data to
12 use their digital computer systems and other devices, such as Personal Data
13 Assistants (PDAs), portable computers and cellular phones as video clip display
14 units to view decrypted multimedia presentations.

15 The invention may be practiced as a method for transmitting and
16 distributing an encrypted video clip file, encrypted in its entirety for security
17 purposes, represented by encrypted data contained in a an encrypted video clip
18 data file. The encrypted multimedia presentation file is transmitted from a file
19 server, which is also able to be broadcast wirelessly via analog and digital RF
20 and other broadcast telecommunication frequencies, to users for display on a
21 digital computer system or other devices with a CPU and output display with
22 audio capabilities, or as a method or apparatus for the display on a video clip

1 display unit of decrypted video clips represented by encrypted data stored in a an
2 encrypted video clip data file.

3 The invention is particularly intended to integrate the secure transmission,
4 broadcast, reception, decryption, playback and display of an encrypted
5 multimedia presentation to end users with personal computers and to those
6 users equipped with devices that have a CPU and a display output with audio
7 capabilities, which facilitates the secure display of decrypted audio, video, still
8 raster images and graphics, still and motion vector images and graphics together
9 with the display of decrypted textual information such as HTML, Rich Text and
10 hyperlinks, relating to the audio, video, and images being displayed, and which
11 all presentation data files can be protected further with encrypted password data
12 and date expiration data.

14 **Brief Description of Drawings**

15 Figure 1 illustrates a system for the distribution and transmission of encrypted video
16 clip data files containing encrypted multimedia component files which comprise an
17 encrypted multimedia presentation file, from a file server to a digital computer
18 system and alternately being wirelessly transmitted and broadcast digitally and
19 analogously to any other device capable of receiving such broadcasts with a CPU,
20 an output display device and an audio output device, to decrypt and playback the
21 interactive multimedia presentation data and files;

1 Figure 2 illustrates the components which comprise a video clip data file that
2 constitute a secure and encrypted multimedia presentation transmission and
3 distribution file;

4
5 Figure 3 illustrates the flow of component data through the respective decoding
6 modules of a video clip display unit within an encrypted multimedia presentation
7 transmission and distribution file;

8
9 Figure 4 illustrates a logical sequence of steps executed by a video clip display unit
10 embodying the present invention to decrypt an encrypted multimedia transmission
11 and distribution presentation file;

12
13 Figure 5 illustrates a logical sequence of steps executed by the decrypted video clip
14 display sequence of a specific embodiment of the present invention;

15
16 Figure 6 illustrates a logical sequence of steps executed by the decrypted text
17 display component of a specific embodiment of the present invention;

18
19 Figure 7 illustrates a video clip user interface capable of playing back non-
20 encrypted multimedia presentations and decrypting and playing back encrypted
21 multimedia presentations displayed by a specific embodiment of the invention.

Detailed Description of the Invention

Figure 1 shows a generic representation of a server-based encrypted video clip data file distribution system and a broadcast wireless file distribution system both of which utilize commonly known digital and analog data transfer technologies. In both distribution systems, a file server having the capacity to store large amounts of binary data holds groups of binary data representing the combined component signals of individual encrypted video clips that contain encrypted multimedia presentations. Using wireless communication systems and devices, such as Personal Data Assistants and cellular telephones, the encrypted multimedia presentation can be sent by one user to other end users without a file server, however, in a wired data transfer system, the file server links and directly transfers the encrypted multimedia presentation file by frame packet relay transmission means to a remote digital computer systems. The wired data transfer system consists of one or more modems, which are attached to the file server which serve as a link between the file server and a telephone system. The modem is a device which is capable of transmitting and receiving an audio-band signal which is representative of binary data. Through the telephone, cable, satellite and wireless telecommunication systems, one modem can communicate such a representative audio signal to another modem, thereby effectively communicating the contents of the encrypted video clip data file which the audio signal represents. A second modem at the end of the data transfer system may then communicate the encrypted video clip data file to the binary data file repository of a digital computer system, comprised of a data storage unit, a data processing unit, and audio and

1 video display units, where the data will be available for subsequent processing and
2 display. In wireless systems the encrypted video clip data containing the encrypted
3 multimedia presentation information, files and data are mass distributed directly
4 using telecommunication frequencies to individual end users of devices such as
5 PDAs, cellular phones and also to television viewers. Alternately, in the wireless
6 system using wireless devices such as PDAs, cellular phones and portable
7 computers, the encrypted multimedia presentation can be sent by one user to other
8 end users without a file server. Future advances in telecommunications technology
9 are expected to facilitate direct communication of digital data, eliminating the need
10 for intermediate modulation and demodulation steps.

11 An encrypted video clip data file contains encrypted multimedia data
12 representative of all of the components of the multimedia presentation video clip file
13 which it represents. Figure 2 shows the component data and information which
14 would be contained in a an encrypted video clip data file representative of video clip
15 data file components comprising an encrypted multimedia presentation consisting
16 of encryption and decryption key data and information, encrypted password data
17 and information, encrypted date and time expiration data and information,
18 encrypted video data and encrypted data file video images, encrypted audio
19 signals, encrypted audio data and encrypted audio data files, encrypted vector still
20 and motion images and graphics data information and files, encrypted still raster
21 image data information and files, encrypted HTML, encrypted hyperlinks, encrypted
22 Rich Text, encrypted ASCII text and other encrypted textually related data
23 information and files and encrypted synchronization data and information.

1 In addition to data representative of the contents of the encrypted video clip, the
2 video clip data file must contain some information which indicates to the video clip
3 display unit how the decrypted video and audio and other decrypted components
4 are to be synchronized as well as how the decrypted multimedia presentation is
5 synchronized. If the decrypted component data are maintained as separate groups
6 of data, the decrypted synchronization information may consist of a separate group
7 of decrypted synchronization data, such as a table which contains data indicating
8 points of temporal correlation between the various decrypted video clip
9 components. The display of a decrypted video clip represented by such data could
10 be implemented through a method such as non-preemptive multitasking, wherein
11 segments of each type of decrypted data are sequentially processed and displayed.
12 Alternatively, some or all of the component data of the decrypted video and audio
13 data and files could be organized in an interleaved data format, which would consist
14 of one or more data files in which segments of the separate component data are
15 arranged and identified serially, in approximately the same order as that in which
16 they would be accessed for display if stored separately. Alternatively, some or all of
17 the component data within the encrypted multimedia presentation file could also be
18 organized in a non-interleaved format.

19 A user wishing to obtain and playback encrypted video clip data files from a
20 file server and through wireless broadcast means must be provided with all of the
21 encrypted component data as shown in Figure 2. This is achieved by transferring
22 the complete secure encrypted multimedia presentation data file instead of
23 insecurely transferring each non-encrypted component data file individually. The

1 optimal way of making this data available is to archive and encrypt any
2 separately maintained component data files into a single encrypted video clip
3 data file identified by a single video clip data file identifier. This may be achieved
4 by using any known archiving and encryption algorithms. Additionally, it is optimal
5 to inform the potential user as to the type and quality of the audio, video, and still
6 image signals which are represented by the component data contained in the
7 encrypted multimedia presentation video clip data file.

8 This may be accomplished by assigning a unique identifier to which is
9 representative of the type and quality of component signals to each component
10 data file. An audio component file type identifier may be used, for example, in
11 conjunction with the eight character file identifier standard of operating systems
12 such as DOS and WINDOWS.

13 When used in conjunction with a file identifier in a systematic and
14 conspicuous manner, such as by systematically incorporating the format identifier
15 as the last two characters of the file identifier, the type and quality of the audio
16 component of the video clip audio may be discerned through reference to a table of
17 file format identifiers. Similar identifiers may be adopted for representation of the
18 component file data types of encrypted video, encrypted still images, encrypted
19 text, and the encrypted interleaved and non-interleaved component data files. File
20 type identification may be accomplished manually or may be automated through
21 the use of a look-up table embodied within the decrypting video clip display
22 playback unit.

1 When audio, video, still images, and text are digitized for storage and
2 distribution, they are typically converted first from analog signals to raw data, and
3 are subsequently compressed or encoded using algorithms which either reduce the
4 amount of information required to represent the respective signal or remove
5 information unnecessary for the regeneration of the respective signal at the desired
6 level of quality. Video clip component data files typically contain data which has
7 been subjected to one or more of such algorithms, and as a result, the video clip
8 display unit must be capable of reversing the compression or encoding process to
9 yield raw video clip component data. This process is carried out by units referred to
10 as decoders or decompression drivers. Figure 3 illustrates the analogous
11 processes which the respective encrypted multimedia presentation video clip
12 component data undergo to yield display-ready decrypted video clip data. Figure 3
13 illustrates these processes as they would be applied to decrypted video clip
14 component data in which the decrypted component data are maintained
15 independently of one another. In an alternative embodiment, in which an
16 interleaved storage format as described above is utilized, for example, a format in
17 which audio and video data are interleaved, the decrypted interleaved data would
18 be processed by a single decompression driver capable of decompressing such
19 data.

20 Figure 4 presents a flow diagram which outlines the basic logical sequence
21 of steps which are executed in a real-time decrypting video clip player apparatus
22 embodying a system component of the invention. The sequence begins by 98
23 determining if the decrypted password and/or date and time information and data

1 and if the decryption or cipher key within the encrypted multimedia presentation is
2 correct. If not, the sequence ends. If correct, the sequence continues by opening
3 the multimedia presentation file for access and then 100 decrypting component files
4 within the encrypted multimedia presentation data file and presenting to a user of a
5 video clip display unit the options of quitting 102 the video display unit, seeking help
6 104 from the unit as to how to operate the unit, or beginning 106 the sequence of
7 steps necessary to display a decrypted video clip multimedia presentation. If the
8 user chooses to begin the display sequence, the video clip display unit accesses its
9 memory and presents 110 the user with a list of data files which the user may
10 attempt to display. Upon the selection of a data file, the file is examined 114 by the
11 video clip player to determine if the decrypted component data files utilize data
12 formats which are compatible with the display unit. If the decrypted files are
13 compatible, the video clip player initiates 116 the execution of a sequence of steps
14 which will result in the display of the decrypted video clip. If the decrypted files are
15 not compatible, an indication of incompatibility is displayed 118 and the user is
16 prompted to make another selection.

17 Figure 5 presents a flow diagram which outlines the basic logical sequence
18 of steps which are executed in the display sequence of a decrypting video clip
19 player embodying the invention. The sequence begins by 121 determining if the
20 decrypted password and/or date and time information and data and if the
21 decryption or cipher key within the encrypted multimedia presentation is correct. If
22 not, the sequence ends 178. If correct, the sequence continues by opening the
23 multimedia presentation file for access and then 121 decrypting component files

1 within the encrypted multimedia presentation data file and writing 120 a video clip
2 display user interface to the display screen of the video clip display unit. The user
3 interface, a specific embodiment of which is illustrated in Figure 7, comprises a
4 decrypted video display area 50 in which decrypted HTML, hyperlinks, Rich Text,
5 ASCII and graphics, as well as decrypted raster still images and graphics and
6 vector still or motion images and graphics, and decrypted video images may be
7 displayed. The user interface further comprises first 52 and second 54 decrypted
8 display areas in which decrypted text, HTML, hyperlinks, Rich Text and graphics
9 components may be displayed. The user interface is further comprised of a user
10 control array 70, which provides the user with controls which allow him to play 60,
11 rewind 62, pause 64, stop 66 the video clip, show sequences of decrypted
12 hyperlinked raster and vector images and graphics 67 and close 68 the video clip
13 player user interface. The user interface is also comprised of a slide bar 58 located
14 within a slide bar area 56 which allows the user to select a position within the
15 decrypted video clip from which display is to be commenced.

16 Once the user interface has been written to the screen of the video clip display unit,
17 a decrypted hyperlinked ASCII, HTML and Rich Text display sequence for
18 displaying the decrypted textual formats within the user interface is initiated 122.
19 The decrypted textual display sequence is discussed at greater length below.

20 Subsequently, a play counter and play position marker are initialized 124. The play
21 counter maintains a record of the number of times that the user has initiated the
22 playing of the decrypted video and audio clip subsequent to selecting it for play and
23 such data along with user demographic IP address client data is reported back to

1 data collection servers. Upon each playing, the play counter is incremented 126.
2 Also upon each playing, the value held by the play counter is examined 128. If the
3 value of the play counter indicates 130 that the play request being responded to is
4 the first of such requests, the video display unit will display 132 any decrypted
5 raster or vector still and motion image and graphic, represented by decrypted raster
6 and vector still and motion image data component in the decrypted video clip data
7 file, for four seconds 134 prior to initiating real-time decryption and decoding 138
8 and display 142 of decrypted audio and video. If the play counter indicates 136 that
9 the play request being responded to is not the first such request, the step of
10 displaying the decrypted still image and decrypted still and motion vector image and
11 graphic is skipped and the decrypted video and audio display sequence is initiated.
12 Subsequent to the decoding 138 of a segment of decrypted audio and video, the
13 play position marker is updated 140 to reflect the relative position within the entire
14 decrypted video clip of the segment of decrypted audio and video to be displayed.
15 A position for the slide bar within the slide bar area which is representative of the
16 relative position of the decrypted audio and video segment being displayed within
17 the decrypted video clip is then calculated 144 using the play position marker, and
18 an updated slide bar is written to the user interface.

19 Subsequent to the initialization 124 of the play counter and play position
20 marker, the display unit repeatedly scans the user control array for requests by
21 the user for the display unit to perform certain predetermined functions.
22 Specifically, the control array is monitored for requests 146 to play the decrypted
23 video clip, for user requests 132 to view a sequence of decrypted still images,

1 still and motion vector images and graphics, for requests 148 to pause the
2 display of the decrypted video clip, for requests 150 to return to the beginning of
3 the decrypted video clip and to recommence play from the beginning of the
4 decrypted video clip, requests 152 to manipulate the position of the play position
5 marker and to thereby select the commencement of display of the decrypted
6 video clip at a particular location within the decrypted video clip, and requests
7 156 to Stop the display of the decrypted video clip. In addition, the display unit
8 repeatedly scans for requests 158 to close the user interface.

9 Upon the detection 162 of a user request to pause the decrypted video
10 clip, the flow of data is halted 164 and scanning of the user interface is resumed.
11 Upon the detection 166 of a user request to rewind the decrypted video clip, the
12 play position marker is reinitialized 168 and the decrypted play sequence is
13 reinitiated. Upon the detection 170 of a user request to manipulate the position of
14 the decrypted video clip segment by means of the slide bar, a new play position
15 marker is calculated 154 based on the user-selected position of the slide bar and
16 play of the decrypted video clip is continued from that updated point. Upon the
17 detection 172 of a user request to stop the display of the decrypted video clip,
18 play is halted and the decrypted textual data files and information represented by
19 decrypted textual data maintained in RAM (described more fully below) is written
20 174 to the decrypted video display area shown in Figure 7, Element 50. Upon the
21 detection 176 of a user request to close the user interface, control of the display
22 unit is returned 178 to the basic sequence as illustrated in Figure 7 and as
23 described above.

1 Figure 6 presents a flow diagram which outlines the basic logical sequence
2 of steps executed in the decrypted text decode and decrypted display sequence of
3 a decrypting video clip player embodying the invention. The decrypted text decode
4 sequence is initiated at the beginning of the decrypted video clip display sequence
5 and begins with a determination 200 of whether the encrypted video clip data file
6 includes data representative of decrypted text to be displayed in synchronization
7 with the decrypted video and audio components of the decrypted video clip. If it is
8 determined 202 that no decrypted text is included in the decrypted video clip,
9 control is returned 204 to end the decrypted video clip display sequence as
10 illustrated in Figure 6.

11 If it is determined 201 that the decrypted date and time is correct and that
12 the decrypted password matches that entered by the end user is correct then the
13 encrypted multimedia presentation file is opened for decryption of the encrypted
14 component files contained within and then 206 that the decrypted video clip data
15 file includes decrypted data representative of decrypted textual information to be
16 displayed in synchronization with the decrypted audio and decrypted video
17 components of the encrypted video clip, then three decrypted text areas in the
18 random access memory (RAM) of the decrypting video display unit are defined 208.
19 A decrypted text counter is then initialized 210.

20 The decrypted text counter serves as a reference which indicates which of
21 the three areas defined in RAM are to receive the decrypted text which is in the
22 process of being decoded. A mark counter is then initialized 212. The mark counter
23 provides a means for detecting marks which serve to demarcate distinct decrypted

1 text data groups which are to be displayed in separate decrypted display areas on
2 the user interface.

3 After the counters are initialized, a character of text is decrypted and
4 decoded 214. If the decrypted character does not indicate 216 that it is the last
5 character within the decrypted text file or data, it is examined 218, 220, 222 to
6 determine whether it is one of a combination of decrypted characters which
7 demarcates the division between decrypted text to be written to different
8 decrypted text areas defined in RAM. If the character does not indicate 224 that
9 further decrypted text should be written to the next decrypted text area in RAM,
10 the decrypted decoded character is written 226 to the area indicated by the
11 decrypted text counter and the following decrypted and encoded text character is
12 decoded 214. If the character does indicate 228 that further decrypted decoded
13 text should be written to the next decrypted text area defined in RAM, the
14 decrypted text counter is incremented 230 and the next decrypted encoded text
15 character is decrypted and decoded 214. When the end of the decrypted textual
16 data and file is reached 232, the decrypted text represented by decrypted text
17 data in each of the three decrypted text areas defined in RAM is written 234 to
18 the three separate decrypted display areas on the user interface and control is
19 returned 236 to the decrypted display sequence as illustrated in Figure 5 and
20 described above.

21 As the sequence of Figure 5 illustrates, the decrypted and then decoded
22 text is the first component of the encrypted multimedia presentation video clip file
23 to be displayed. Decrypted text, again which may consist of HTML, Rich Text,

1 hyperlinks and ASCII, stored as decrypted text data in the first RAM decrypted
2 text area is displayed in the decrypted video display area 50, decrypted text
3 stored as decrypted textual data in the second RAM decrypted text area is
4 displayed in the first decrypted text display area 52, and decrypted text stored as
5 decrypted text data in the third RAM decrypted text area is displayed in the
6 second decrypted text area 54. When the decrypted video clip is played 60, and
7 when images 67 are displayed, decrypted text displayed in the decrypted video
8 display area 50 is overwritten by decrypted raster and vector still and motion
9 images or decrypted video images. However, because the decrypted and
10 decoded text is maintained in RAM for as long as the decrypted multimedia
11 presentation clip remains active within the video clip multimedia presentation
12 display unit, the decrypted textual data and information initially displayed in the
13 decrypted video display area 50 may be redisplayed upon completion of play of
14 the decrypted video clip, while decrypted text, HTML, Rich Text, hyperlinks,
15 ASCII and decrypted images and graphics displayed in the decrypted text
16 display areas 52 and 54 of the user interface remains displayed throughout the
17 entirety of the display of the decrypted video clip.

19 **Specific Embodiment and Best Mode of the Invention**

20 The information disclosed hereinafter, in combination with the detailed
21 description of the invention provided above, describes a specific embodiment of the
22 invention. This embodiment of the invention is the best mode of the invention
23 known to the inventors as of the date of the filing of this application.

1 This embodiment of the invention implements the disclosed process as computer
2 software and utilizes a personal computer and other devices with a CPU, output
3 display and audio capabilities, to display the encrypted multimedia presentation as
4 the decrypted video clip display apparatus. It is optimized for use by a user of a
5 personal computer and users of other devices with a CPU, output display and audio
6 capabilities which is capable of running WINDOWS applications and other
7 computer operating systems and which includes a modem capable of accessing
8 computer network services such as the Internet or analogous subscription services
9 such as America On Line (AOL). Alternately the invention decrypts and displays
10 received encrypted multimedia presentation transmission files through intranets or
11 LANs, wide area networks and other such networks, and such encrypted
12 multimedia presentation files are also broadcast wirelessly to users of other devices
13 equipped with wireless modems and antennas, such as PDAs, cellular phones, and
14 portable computer systems. Further the encrypted multimedia presentation file is
15 transmitted and broadcast using known telecommunication frequencies to CPU
16 equipped set top decoders boxes via digital and analog satellite and cable means
17 for television playback. Computer code facilitating the practice of this embodiment
18 of the invention for such a system is available as a microfiche appendix to U.S.
19 Patent No. 5,983,236. The code consists of five modules which are written in the
20 C++ computing language and in this embodiment are designed for use as
21 WINDOWS applications and with translation, functions in other operating systems
22 and program languages. The particular function of each module is described in
23 headers provided at the top of each of the microfiched pages.

1 The decrypted video display process is preceded by acquisition of secure
2 encrypted multimedia presentation video clip data files by the user. This is
3 accomplished by establishing a connection between the computer and a computer
4 network service such as the Internet, the process of which is well known. The user
5 then uses well known searching techniques to locate files which are compatible
6 with the decrypting multimedia presentation video clip player which is implemented
7 on the user's personal computer and other such CPU equipped devices. This
8 process is facilitated by assigning a unique two to three character file identifier
9 extension to a single encrypted video clip data file which consists of the encrypted
10 component data files joined in a single data file through the use of any well known
11 archiving format such as LHARC, PK-ZIP, PGP encryption and other such
12 archiving and encryption/decryption processes. Alternately, the end user may
13 acquire the encrypted multimedia presentation video clip file through devices
14 connected to the Internet wirelessly or directly from other user of such devices
15 known as personal data assistants (PDAs) or cellular phones or other broadcast
16 means using known telecommunication and broadcast frequencies. The encrypted
17 multimedia presentation data file may also be shared without a file server between
18 users, using either wired and wireless connections, through peer-to-peer file
19 sharing networks.

20 The encrypted multimedia presentation video clip data file distribution and
21 transmission process is further facilitated by assigning component data file
22 identifiers which convey information as to the data format in which the encrypted
23 video clip components are represented. In the present embodiment, this is

1 accomplished by reserving the last three characters within the standard eight
2 character file identifier for a three character code which reflects the type and quality
3 of the audio signal represented therein. Combining these features, a user seeing
4 that the audio portion of the encrypted video clip data file is identified, for example,
5 as NAME.M3X, would recognize that the file is an audio data file which is
6 representative of a stereo audio signal sampled at 192 bit rate samples per
7 channel, having a frequency range of 44.1 kHz, a compression ratio of 4.5:1, and
8 which is encoded using the MPEG 3 Audio standard with a 128 KBPS output or
9 streaming data rate. Analogous naming conventions may be established for all
10 component data files.

11 Subsequent to the transfer of the component data files of an encrypted video
12 clip data file from any one of the methods above, including from a file server or
13 broadcast point to the storage device of the user's personal computer and memory
14 of a wireless device, such processes being well known, the user may initiate the
15 decryption and display of the encrypted video clip represented by the encrypted
16 video clip data file by means of the process and apparatus disclosed herein. In the
17 specific embodiment and best mode of the invention, this is achieved by a
18 decrypting multimedia presentation video clip player implemented through
19 computer code executed on the user's personal computer and other CPU enabled
20 devices and their particular operating system. The code executes the sequences of
21 steps described above and in Figures 4 through 6, operating on data of the type
22 represented by Figure 2 and in the manner illustrated by Figure 3.

1 As one example, to allow a personal computer to display the various
2 components of an encrypted multimedia presentation file video clip, the encrypted
3 video clip data must be processed in a manner which decrypts and converts the
4 encrypted component data into forms which are displayable by the computer. This
5 requires decompression or decoding of the decrypted data as illustrated in Figure 3.
6 In the specific embodiment and best mode of the invention, the personal computer
7 is programmed with an installed CODEC (compression and decompression
8 program or method) to decompress and display decrypted video data stored in any
9 one of a number of formats such as MPEG, AVI, QuickTime, DivX, WMV, ASF or
10 other well known compression/decompression formats. The MPEG video data
11 formats and other formats are well known video data formats which were
12 developed and promulgated by the Moving Pictures Expert Group, while the .AVI,
13 .WMV and .ASF formats were developed and promulgated by Microsoft and the
14 QuickTime .MOV format developed and promulgated by Apple Computer.
15 Consequently, the video decompression driver of the present embodiment as
16 illustrated in Figure 3 is a computer-implemented MPEG decompression driver
17 which receives data in a number of MPEG formats and converts it to data in the
18 Device Independent Bitmap (DIB) format. The DIB format is compatible with the
19 display logic and circuitry found in personal computers as well as other devices
20 equipped with a CPU, output display and audio capabilities such as PDAs or
21 cellular phones. Computer and CPU implemented MPEG decompression drivers
22 may be found, for example, as a standard component within computer operating
23 system software packages, however, a host of various audio and video

1 decompression drivers come prepackaged and preinstalled with many of today's
2 computer systems and devices. Many more decompression drivers for various
3 video and audio formats can be freely found and downloaded from the Internet,
4 often at little to zero cost. For purposes of compatibility recognition, encrypted
5 video component data files compatible with this embodiment of the invention are
6 assigned the file identifier extension .NMS and other such unique identifiers.

7 Similarly, the specific embodiment and best mode of the invention is
8 configured to first encrypt, decrypt and then decode audio data represented by data
9 stored in the .WAV (WINDOWS AUDIO), .WMA, .MP2, .MP3 and other file formats
10 commonly used for encoding digital audio. Decompression decoders for audio data
11 stored in these and other formats are most often found in computer software
12 operating systems distributed by the MICROSOFT Corporation or can be easily
13 found on the Internet from other developers. All digital audio formats use the
14 decoded audio data as a digitized data stream which may be converted by means
15 of an analog to digital (A/D) converter into an audio signal.

16 Simultaneous decrypting, decoding and display of the audio and video
17 components is implemented through the well known method of non-preemptive
18 multitasking, such as is facilitated by the WINDOWS operating system, and other
19 operating systems such as LINUX or those used on CPU equipped devices with
20 output displays and audio capabilities such as found in personal data assistants
21 (PDAs) and cellular phones, which function using WINDOWS CE and other
22 operating systems. For purposes of compatibility recognition, audio component
23 data files compatible with this embodiment of the invention are assigned the file

1 identifier extension .WAV, however the invention is also functional using many
2 other audio component data file formats such as .MP2, .MP3, .WMA, etcetera.
3 The specific embodiment of the invention also is configured to decode still image
4 data stored in the .JPEG, .JPG, .BMP, .PNG, and other raster graphic still image
5 data formats as well as both still and motion vector image formats such as those
6 formulated by Macromedia using their .FLA Flash graphics formats. JPEG is
7 formulated and distributed by a subdivision of the makers of the MPEG video data
8 formats, the Joint Photographic Expert Group, and JPEG decoders are well known.
9 For purposes of compatibility recognition, still image component data files
10 compatible with this embodiment of the invention are assigned the file identifier
11 extension .NIM, however, in other embodiments and practical application, the
12 invention decrypts and decodes many other image and graphic formats with
13 extensions other than .NIM alone, as noted above.

14 While the above formats are presently supported in the specific embodiment
15 and best mode of the invention, the disclosure provided herein will suggest
16 alternative embodiments to those skilled in art of digital audio and video processing.
17 Alternative audio and video data formats may be supported by substituting the
18 proper decompression or decoding algorithms. For example, a decoder of still
19 image data adapted for use with the .GIF, .TIF and .BMP formats could be
20 substituted for the JPEG decoder of the present embodiment. Alternatively, multiple
21 decompression drivers could be substituted which are capable of processing,
22 decompressing and decoding audio and video data stored in both interleaved and
23 non-interleaved formats. Examples of such interleaved and non-interleaved formats

1 are .AVI (AUDIO VIDEO INTERLEAVE), .ASF and .WMV, produced by the
2 MICROSOFT Corporation and MPEG2, produced by the Moving Pictures Expert
3 Group.
4 Similarly, there are numerous well-known methods for the compression or encoding
5 of ASCII text, HTML with hyperlinks, .RTF Rich Text and other such textual data
6 which may be implemented. The present embodiment of the invention uses a
7 simple mathematical alteration of any one of these textual data formats which is
8 reversed upon decrypting and decoding. This alteration, along with encryption and
9 decryption of the encrypted multimedia presentation data file, involves the
10 permutation of each data word representing each textual character by the addition
11 of a fixed four byte revolving key. This encoding does not change the length of the
12 file. Decryption involves the simple subtraction of this same fixed revolving key from
13 each character in the encrypted file and encrypted data files. Alternatively,
14 decoding modules configured for use with any of the well-known encryption
15 methods may be similarly adapted. For purposes of compatibility recognition, text
16 component data files compatible with this embodiment of the invention are
17 assigned the file identifier extension .NTX, .HTM, .HTML, .SHTML, .RTF, .RTX,
18 .TXT and other text file format extensions.

19 Figure 7 illustrates the video display unit user interface of the present
20 embodiment of the invention for decrypting and displaying a secure interactive
21 multimedia presentation. The interface is designed to be intuitively useable by
22 users who are familiar with the WINDOWS style user interface and operating
23 system and may be practiced using non-WINDOWS operating systems on CPU

1 enabled devices. The user interface includes a large decrypted video display area
2 50 having a resolution at startup of 320 pixels x 240 pixels. The user interface,
3 however, can also display decrypted video at 160 pixels x 120 pixels as well as
4 display decrypted video at full screen mode, which in this display mode, effectively
5 hides the user interface in its entirety. The user interface auto-redisplays when
6 decrypted video clip playback is stopped manually by the user or when the
7 decrypted video clip has reach the end point of the video clip. Below the decrypted
8 video display area are situated a first decrypted textual data and graphical data
9 display area 52 and a second decrypted textual data display and graphical data
10 display area 54. Between the decrypted textual and graphical display areas and the
11 decrypted video display area is the slide bar area 56 which includes a slide bar 58
12 for performing the functions described above. To the right of the video display area
13 is the user control array 70 which includes a play button 60, rewind button 62,
14 pause button 64, stop button 66, images display button 67, and close button 68.
15 These buttons are intended to be operated by the user with the assistance of a
16 mouse-directed pointer. The methods of such use and the technology for its
17 implementation are well known in the art of computer programming.

18 Prior to the decrypted audio and video decoding sequence, the decrypting
19 multimedia presentation video player's user interface of the present embodiment
20 decrypts, decodes and displays decrypted textual and graphical information at
21 startup of the user interface. The decrypted textual information and data is
22 examined for markers which indicate points of demarcation between groups of
23 decrypted text data representing groups of decrypted textual data and information

1 in any one of the above noted textual formats and decrypted graphical data and
2 information to be displayed in separate display areas. In practice it has been found
3 that two consecutive characters such as "@@" and other such textual markers are
4 sufficient to provide such demarcation. Figure 6 illustrates the use of a counter
5 which is referred to 220 to determine whether a point of demarcation has been
6 detected. This serves to indicate that subsequent decrypted text should be written
7 224 to the next decrypted text area defined in RAM, until such time as a further
8 demarcation point is detected.